Improving Our Odds: Success through Continuous Risk Management

Phillip O. Greenhalgh, CSP; Project Engineer, ATK Launch Systems Inc., Brigham City, Utah, USA

Keywords: Risk Identification, Assessment and Mitigation, Risk-based Design, Risk Management Tools

Abstract

Launching a rocket, running a business, driving to work and even day-to-day living all involve some degree of risk. Risk is ever present yet not always recognized, adequately assessed and appropriately mitigated. Identification, assessment and mitigation of risk are elements of the risk management component of the "continuous improvement" way of life that has become a hallmark of successful and progressive enterprises. While the application of risk management techniques to provide continuous improvement may be detailed and extensive, the philosophy, ideals and tools can be beneficially applied to all situations. Experiences with the use of risk identification, assessment and mitigation techniques for complex systems and processes are described. System safety efforts and tools used to examine potential risks of the Ares I First Stage of NASA's new Constellation Crew Launch Vehicle (CLV) presently being designed are noted as examples. Recommendations from lessons learned are provided for the application of risk management during the development of new systems as well as for the improvement of existing systems. Lessons learned and suggestions given are also examined for applicability to simple systems, uncomplicated processes and routine personal daily tasks. This paper informs the reader of varied uses of risk management efforts and techniques to identify, assess and mitigate risk for improvement of products, success of business, protection of people and enhancement of personal life.

Introduction

Launching a rocket, running a business, flying in an airplane, operating machinery, driving to work, even crossing the street all involve some degree of risk. Indeed, life itself is risky business as all of us run the risk of dying of old age if nothing else "gets us" first. Risk, defined as "the possibility of suffering harm or loss" (ref. 1), is ever present to some extent in everything we do, yet we do not always recognize what risks we face. Sometimes we recognize risk but fail to take steps to mitigate that risk even though the consequences may be significant. Recent events relevant to economic conditions remind us of the financial risks to individuals, corporations, governments and even insurance institutions that exist for the mitigation of potential risk. As each risk we face has the two components of uncertainty and loss (ref. 2), we should structure our efforts to lessen either or both components thereby improving the odds we can avoid the potential resultant loss or harm.

Risk management is the structure for dealing with risk, be it intentional and involved or subconscious and simple. Risk management is "a discipline for living with the possibility that future events may cause adverse effects" (ref. 3). To persons in different situations, risk management takes on a different emphasis, yet the basics are the same. Those in the financial industry have traditionally used sophisticated techniques including processes like currency hedging and interest rate swaps. A project manager's effort includes a focus on assuring the accurate tracking of schedules and costs to assure a project is on time and within budget. In the insurance industry, risk management is accomplished by coordination of insurable risks and reduction of expenses. Safety professionals work to reduce accidents and injuries on the job. Engineers designing rockets for manned space flight design with risk in mind seeking to eliminate or mitigate risk before beginning to build. Continuous risk management (CRM) then is risk management for risks that are assessed on an ongoing basis and used for decision making in all phases of a project. CRM carries the risk forward and deals with it until it is resolved or until it turns into a problem with subsequent loss (ref. 4). With risks present at all times in every aspect of life, the implementation of the principles of CRM improves our odds of success and avoidance of problems by reducing the likelihood of occurrence and/or the severity of consequences of suffering harm or loss.

Elements of the CRM Process

Improving our odds for success with CRM involves the continual use of the steps: identify, analyze, plan, track and control all the while communicating the risk (Figure 1).

Figure 1 – CRM Process (ref. 5)

- Identify – find the risks before they can become problems and result in loss or harm. A process of realizing the uncertainty for loss or harm
  - Capture the statement of risk in a way it can be described and measured
    - Given the (condition) there is a potential that (risk) could result in (consequence) . . .
  - Capture the context of risk
    - Include additional information relevant to the circumstances surrounding the identified risk
  - Communicate the identified risk
- Analyze – process of examining the risk in order to tell the potential extent, severity and likelihood
  - Evaluate the attributes of risks
    - Impact
    - Probability
    - Timeframe
  - Classify the risks
    - Grouping of risks based on similar characteristics
  - Prioritize the risks
    - Ranking of risks to define those most significant or those that need the most attention
  - Communicate the results or status of the analysis
- Plan – decide what to do with risks and how to go about doing it
  - Plan risk mitigation activities
  - Assign responsibilities
  - Communicate what is happening with the risk and how it is going
- Track – follow the risk and the assigned risk responsibilities, collect more information
  - Monitor the risk and all related actions
  - Provide status reports
  - Communicate information relative to the progress of the risk
- Control – executing the risk mitigation activities that will reduce risks to levels where the uncertainties (likelihood) and potential loss (severity) are reduced to an acceptable level
  - Implement the controls
  - Monitor the controls
  - Communicate the effectiveness of the controls

Communication is the centerpiece that holds the CRM process together. It is present in each of the steps and, as Figure 1 depicts, it holds all of the steps together as a central hub. Without communication, the process quickly loses value (ref. 6).

Application of the CRM Process in the Simple and the Complex

The philosophy and ideals of CRM can be beneficially applied to all situations. While the application of risk management techniques may be detailed and extensive for complex systems, application of some or all of the principles of CRM are often applied in our every-day lives without realizing we are doing so.

A Very Simple, Real Life Example Provides an Illustration of Improving the Odds With CRM: A mother identifies that given the proximity of a nearby street, there is a potential for her little child to run into that street with the subsequent possibility the child could be struck by a passing vehicle resulting in severe injury or death. In an instant, the mother analyzes the situation and, with concern for the safety of the child, determines the child must be kept from the street. The mother acts immediately with her plan to mitigate the risk presented by the nearby street as she separates the child from the hazard. Immediate plans include holding the child when outside to physically prevent the child from nearing the street. Additional plans include a fence and gate with a lock to provide a physical barrier between the child and the street as well as constant monitoring of the child's outside activity. Over time as the child grows old enough, the plans progress until eventually including teaching the child about the street and how to be safe when near it and even how to cross it safely. All the while, the mitigation plans are being made and enacted; the mother tracks the child continually, verifying that the controls that were put in place are always effective. The mother is also constantly vigilant and ready to intervene if a weakness is found. While the mother has gone through each of the CRM steps and identified, analyzed, planned, tracked and controlled to the extent possible the risk the street presents to a child, she has continually communicated with the child the danger of the street. Communication of the risk began with physical restraint and stern warnings of the street, then restrictions to remain within an allowed boundary as the hazard mitigating barriers were put in place, then later the child was taught how to be safe when near a street.

Example of Complex Systems and Processes Using Basic Principles of CRM Applied for the Reduction of Inherent Risks (improving the odds): CRM principles and philosophies are used in launching rockets for manned space flight. Even though formal tools, systems and processes are used to identify, analyze, plan, track, control and communicate, the same CRM principles are used. NASA Space Shuttle Program Manager Wayne Hale has said concerning all involved in any way with each shuttle mission, "Our collective job is to understand the risk, mitigate it as much as possible, communicate accurately all around about the risk remaining, and then decide if we can go on with that risk" (ref.7). ATK Launch Systems Inc. uses this philosophy employing a comprehensive CRM effort in managing the risks of a complex system on NASA's Constellation program, the next generation of manned space vehicles presently in the design stage.

In designing the Ares I First Stage launch vehicle, part of the overall Constellation CLV, the risk management process has been employed from the initial design stages. Program and project teams are responsible for identifying, analyzing, planning, tracking, controlling, mitigating and communicating risks using a number of risk management tools as depicted in Figure 2. Risk management is a continuous, iterative process to manage risk in order to achieve program and mission success, it is a key element and an integral part of normal program and project management and engineering processes.

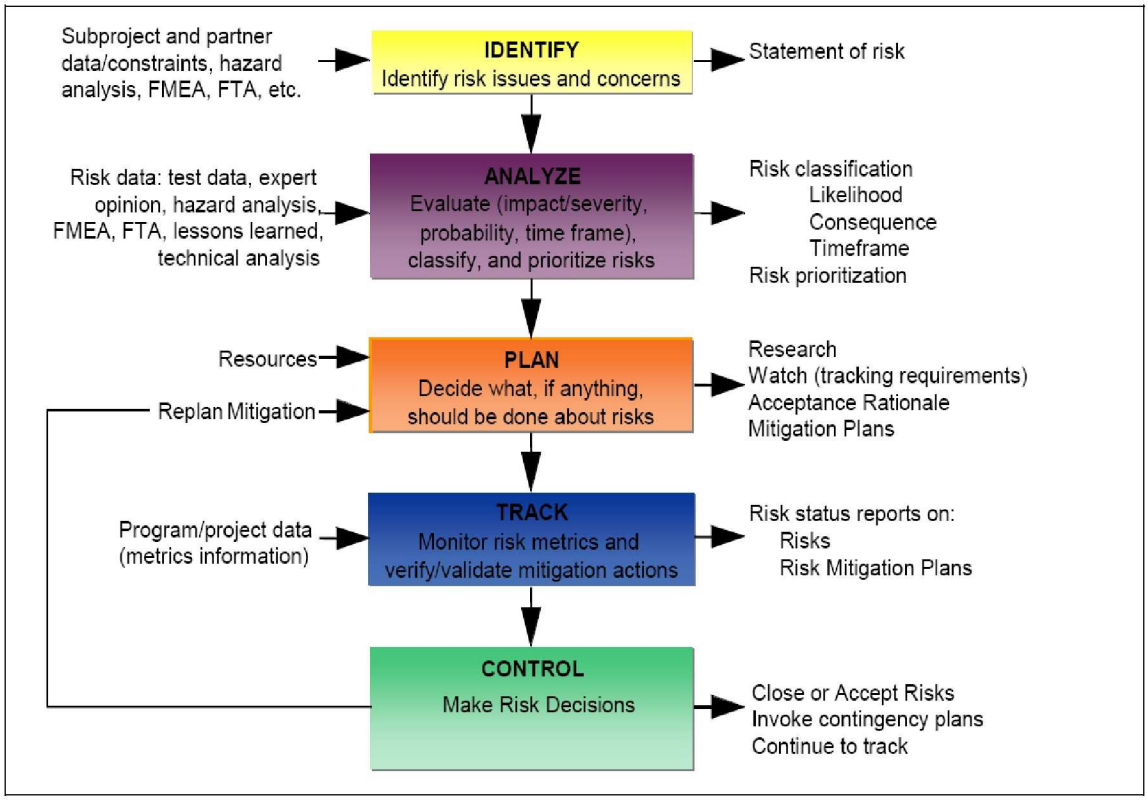


Figure 2 – CRM Process Flow (ref. 8)

Under the umbrella of CRM (Figure 3), a complete array of system safety and reliability tools are used by ATK Launch Systems to identify risks to flight through all life cycle phases.

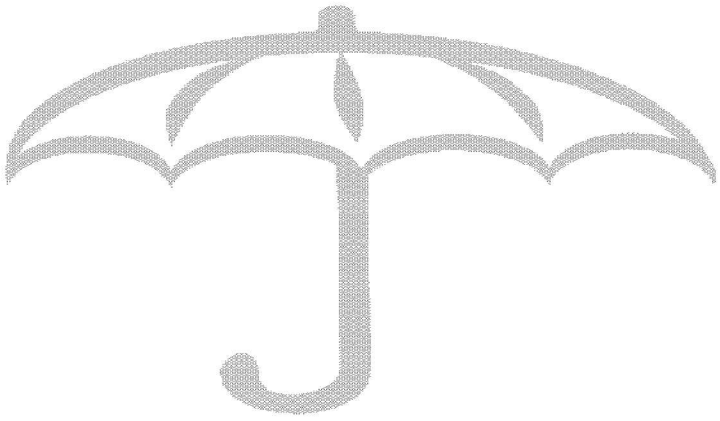


Figure 3 – System Safety and Reliability Tools

Continuous, Life Cycle Risk Management: Risk-based Design
Program Risk, Product Hardware Risk, Process Risk, Support Process Risk
Facility and Process Risk, Supplier Risks, Other Risks

Risk Management Tools: Fault Tree Analysis, Hazard Analysis,
Failure Modes and Effects Analysis/Critical Items List, Probabilistic Risk Assessment,
Lessons Learned, Brainstorming, etc.

Risk-based Design: The CRM process used for ATK Launch Systems Inc. Ares I First Stage Project for the Constellation program began with risk-based design (RBD). RBD is a structured, formalized methodology in which risk consideration becomes an integral part of the initial design process. The objective of RBD is to identify and characterize risks during the concept development and preliminary design phases and communicate the risks with all involved. As risks are identified and characterized, planning as to how to handle each risk is accomplished. The first effort is to design out risks during these preliminary design phases. If it is not possible to design out risk, risk mitigation techniques are applied to provide failure tolerance (i.e. redundancy). When designing in failure tolerance is not possible or is prohibitive to the function of the system, efforts are then focused to design for minimum risk (i.e. safety factors). If all efforts to address reduction of risk are not able to provide the desired improvement of bringing the risk to an acceptable level, decisions are made to determine if there will be an acceptance of risk at that present level or if it is "back to the drawing boards" for redesign. RBD involves the integration of design engineering and project management with system safety, reliability, maintainability, supportability, manufacturability, operability and affordability. Again the key to developing a RBD activity is the integration and communication of risk identification and characterization within the design process. The early identification of risks provides the opportunity to prioritize the allocation of resources based on the reduction of overall system risk. Where applicable, RBD efforts use hazard analyses, fault tree analyses (FTA) and failure modes and effects analysis (FMEA). NASA's Constellation design process includes RBD activities at all design levels from the component to the subsystem to the system to the stage or element level (i.e. Ares I First Stage) to the Ares system level (propulsion elements) and the Orion system level (Crew elements) to the overall Constellation system. Where dominate failure modes cannot be designed out, the design incorporates specific provisions to address the points of risk. Such provision may include, but are not limited to, critical inspections, operating constraints, monitoring systems and relief provisions.

Application of Risk Management Tools in Identifying, Assessing, Controlling and Verifying the Risks

Hazard Analyses: The use of hazard analyses is applied as a primary CRM effort used in an iterative manner. Beginning with the preliminary hazard analyses, an examination of the design is provided to identify potential hazards and hazard causes at a time when the design can be influenced and adjustments made to eliminate risks. As the design matures, a subsystem hazard analyses is provided with controls that are identified for all residual risks that could not be eliminated. The hazard analyses process continues to evolve with verification of controls through testing, analysis and inspection of the design features. The hazard analyses become an ongoing examination of risks to the flight article through all phases from manufacture through flight and the subsequent refurbishment and reuse of hardware where applicable (ref. 9). Included with each hazard analysis is a risk matrix giving a visual depiction of the estimation of relative risk with the hazardous condition in each report and the subsequent causes identified. The risk matrix used by all Constellation element hazard analyses is defined by NASA in Constellation Project document CxP 70038 and serves well as a discussion tool frequently used to fully vet the risk analyzed in each hazard report. A similar risk classification matrix with red, yellow and green denoting high, medium and low risk (Figure 4) is directed for use in the CRM process by another NASA document, CxP 72019.

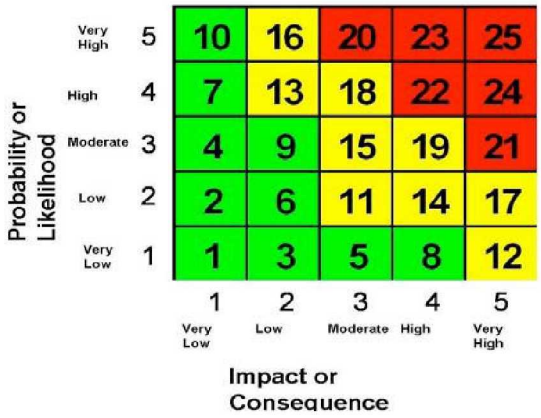


Figure 4 – Risk Classification Matrix (ref. 10)

FTA: Preparation of a FTA of a system is used to identify hazardous conditions and their applicable causes. The FTA is a system safety analysis technique which results in the following: 1) a logic tree developed using deductive logic from a top-level, undesired event to all sub-events which could occur to cause the top event, 2) a graphic representation of the various combinations of possible events along with the interrelationships of system events and their dependence upon each other, and 3) identification of possible cause events and determination of where controls should be applied to assure that the undesired event will not occur. For the Ares I First Stage, the FTA is developed to the level of detail at which controls may be implemented thereby reducing the probability of loss of life or loss of the Constellation system. The FTA has been used to identify the events, hazardous conditions and the hazard causes that are addressed in each of the Ares I First Stage hazard reports.

FMEA/Critical Items List): The FMEA is used to identify potential failure modes of a part, component, or subsystem and denote those where the occurrence would be critical or catastrophic. The Critical Items List (CIL) provides the justification, frequently termed retention rationale, that explains how each particular failure mode is controlled to an acceptable level. Hardware parts, components and subsystems are individually analyzed to determine possible failure modes and what occurrences such as process failures, material defects, etc. could cause a failure. The resulting worst-case effect of each failure mode is then assessed and documented. Using the determined worst-case effects, all items are classified according to an associated failure criticality.

Criticality 1 – Single failure that could result in loss of life or vehicle
Criticality 1R – Redundant hardware item(s), all of which, if failed, could cause loss of life or vehicle
Criticality 1S – Failure in a safety or hazard monitoring hardware item that could cause the system to fail to detect, combat, or operate when needed during a hazardous condition, potentially resulting in loss of life or vehicle
Criticality 2 – Single item failure that could result in loss of mission without loss of life
Criticality 2R – Redundant hardware item(s), all of which, if failed, could cause loss of mission
Criticality 3 – All failures that do not result in loss of life or loss of ability to complete the mission (ref. 11)

For the ATK Launch Systems Inc. Ares I First Stage of the overall Constellation system, the CIL is documented and maintained for all criticality 1, 1R, 1S, 2 and 2R failure modes. The CIL retention rationale documents how each component, material or hardware item is certified and what design safety margins are included. The CIL retention rationale also lists the inspections and tests performed during manufacturing and assembly processes that assure all potential failure causes are controlled and that the controls are verified. Each inspection or test listed in the CIL retention rationale is given a CIL code. These same inspections or tests with the corresponding CIL code are attached to the respective manufacturing test or inspection that is found in the manufacturing and inspection plans. CIL inspections and tests in manufacturing planning cannot be removed or changed without an assessment of risk, changing the CIL retention rationale as applicable, and the subsequent review and approval from ATK Launch Systems Inc. management and NASA. Regular audits of manufacturing planning are conducted by a system safety engineer to verify that all the inspections listed in the CIL are properly called out in the planning. This process ensures that building the Ares I First Stage to design will be repeatable and that documented retention rationale will assure controls are in place so that potential failure modes will not occur (ref. 12).

Probabilistic Risk Assessment (PRA): ATK Launch Systems defines PRA similar to others as "a comprehensive, structured, and logical analysis methodology aimed at identifying and assessing risks one at a time in complex technological systems". PRA generally used for high reliability failure modes that present significant system consequence is targeted at risk environments relative to the system that may involve the compromise of safety, inclusive of the potential loss of life, personal injury and loss or degradation of high-value property. PRA has become a principal analytical methodology for identifying and analyzing technical and safety risk associated with complex systems, projects and programs such as the Ares I First Stage of the Constellation program. The ATK Launch Systems, Ares I First Stage Reliability Plan says: "PRA feeds into and supports the risk management activities by identifying dominant contributors (those events that contribute most to risk) so that resources can be allocated to significant risk drivers and not wasted on items that insignificantly affect overall system risk. PRA provides a framework to quantify uncertainties in events that are important to system safety. By requiring the quantification of uncertainty, PRA informs the decision-makers of the sources of uncertainty and provides information that determines the worth of investing resources to reduce uncertainty. PRA differs from reliability analysis in three important respects: 1) PRA tends to focus on the evaluation of system failure while reliability analysis tends to focus on the evaluation of system success, 2) PRA explicitly quantifies uncertainty while reliability

analysis nominally considers uncertainty in parameter estimates, and 3) PRA quantifies metrics related to the occurrence of highly adverse consequences (e.g., fatalities, illness, loss of mission) as opposed to narrower system performance metrics such as system reliability. PRA also differs from hazard analysis, which evaluates metrics related to the effects of high consequence and low probability events treating them as if they have already occurred. PRA results are directly applicable to resource allocation and other kinds of risk management decision-making based on its broader consequence metrics".

The PRA process is helpful in the identification of weaknesses and vulnerabilities in systems that have the potential to adversely impact the safety, performance and mission success of the system. Such information provides insights for viable risk management strategies for use in the reduction of risk and assists the decision-maker determine where the expenditure of resources can most effectively be utilized in improving the design and operation in the most cost-beneficial manner. The ATK Launch Systems, Ares I First Stage Reliability Plan also states: "The most useful applications of PRA have been in the evaluation of complex systems subject to high-consequence events and the evaluation of complex scenarios consisting of chains of less critical or insignificant events, that when combined interact in a way that leads to a major system failure. Credible chain reaction failures are difficult to identify. Thousands even tens of thousands of such scenarios can be formulated, but which of these are credible? Few tools are available for such what-if analysis. Of these few tools, PRA analysis is perhaps the most useful".

CRM Process: The risk management process for the Ares I First Stage program within ATK Launch Systems Inc. is applied as a means to anticipate, mitigate and control risks and to focus resources where they can be most effectively used to ensure overall success of the program. While the risks addressed through the hazard analyses, FTA, FMEA/CIL and PRA tools are focused at the end item product, the CRM process is utilized to look at all risks. The CRM process has been effectively initiated on the Ares I First Stage program beginning with preliminary design concepts and has been utilized for working cost, schedule, technical and safety risks.

Ares I First Stage identified risks are subjected to the CRM process and are characterized utilizing the Ares risk scorecard shown in Figure 5. After risks are properly defined and scored, a determination is made on the mitigation necessary to reduce the risk to an acceptable level. Usually risks are prioritized based on their relative standing with other risks as ranked by likelihood and severity scores. The goal of risk management is, as a matter of efficiency, to apply resources where they will have the greatest potential of reducing significant program risks. With the risks scored, the overall significance is easily seen in descending significance from red to yellow then green. At times, elevation is required to ensure that significant risks are communicated up the line of management and that needed direction or resources are obtained for mitigation. As each risk has an owner, that person is required to monitor and update mitigation plans showing completion or changes as well as provide a status at periodic risk reviews. As the risk mitigation plan is being fulfilled, the reduction in risk can be depicted with a waterfall chart as shown in the example in Figure 6. In addition to the risk management steps of identify, analyze, plan, track and control, the risk management process for complex systems such as the Ares I First Stage program includes some formal opportunities for documenting and communicating the risk including:

- Risks are identified and documented
- Significant risks (red and yellow at a minimum) are documented in the risk tracking database
- Each risk owner manages his risks
- A Risk Management Board (RMB) reviews new and high (red) risks and others needing special attention as necessary
- The RMB elevates red risks and those needing external resources to the appropriate entity

Reasons for elevating a risk could be: 1) visibility to provide management insight, 2) a higher level assistance is needed from the next higher level of management to share ownership and be able to carry out effective mitigation, and 3) coordination is needed with other organizations and stakeholders. The risk owners are the persons that identify risks requiring elevation.

Consequence (Impact) Rating

Impact		Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Safety	Personnel	No injury or illness to public, crew or personnel	Minor first aid treatment (does not adversely affect personal safety or health)	Medical treatment for an injury or incapacitation	Severe injury or incapacitation	Death or permanent disability
	Assets	Damage to minor asset	Minor loss or damage to facility, system, equipment, or flight hardware	Moderate loss or damage to facility, system, equipment, or flight hardware without impact to mission success	Major loss or damage to facility, system, equipment, or flight hardware with impact to mission success	Loss of vehicle or critical asset which prevents mission success
Performance (Mission Success)	Requirements	Negligible impact to requirements or design margins	Minor impact to requirements or design margins	Moderate impact to requirements or design margins	Major impact to requirements or design margins	Technical goals not achievable with existing engineering capabilities or technologies
	Operations	Negligible impact to mission objectives or operations	Minor impact to operations ± workarounds available	Moderate impact to operations ± workarounds available	Major impact to operations ± workarounds not available	Unable to achieve major mission objectives
	Supportability	Temporary usage loss or capability to maintain a nonflight critical asset	Permanent usage loss or capability to maintain a nonflight critical asset	Temporary usage loss or capability to maintain major element(s) of flight vehicle or ground facility	Permanent usage loss or capability to maintain major element(s) of flight vehicle or ground facility	Inability to support further ESMD flight operations
Cost		≤ 2% overrun to the annual budget or ETC authorized for the general activity	> 2% but ≤ 5% overrun to the annual budget or ETC authorized for the general activity	> 5% but ≤ 10% overrun to the annual budget or ETC authorized for the general activity	> 10% but ≤ 15% overrun to the annual budget or ETC authorized for the general activity	> 15% overrun to the annual budget or ETC authorized for the general activity
Schedule		Negligible or NO schedule impact	Some overall schedule impact; additional activities may be required to meet key dates (no impact to critical path)	≤ 1 month impact to program critical milestones (critical path)	> 1 month impact to program critical milestones (critical path)	Cannot meet program critical milestones

Likelihood (Probability) of Occurrence Rating

Probability Rating (P)	Value	Description
Very High	5	**Qualitative:** Nearly certain to occur, requires immediate management attention; controls have little or no effect **Quantitative:** $10^{-2} < P \leq 10^{-1}$ for risks with primary impact on safety or 50% < P ≤ 100% for risks with primary impact on cost, schedule or performance
High	4	**Qualitative:** Highly likely to occur, most cases require management attention; controls have significant uncertainties **Quantitative:** $10^{-3} < P \leq 10^{-2}$ for risks with primary impact on safety or 33% < P ≤ 50% for risks with primary impact on cost, schedule or performance
Moderate	3	**Qualitative:** May occur, management required in some cases; controls exist with some uncertainties **Quantitative:** $10^{-4} < P \leq 10^{-3}$ for risk with primary impact on safety or 10% < P ≤ 33% for risks with primary impact on cost, schedule or performance
Low	2	**Qualitative:** Not likely to occur, management not required in most cases; controls have minor limitations/ uncertainties **Quantitative:** $10^{-5} < P \leq 10^{-4}$ for risks with primary impact on safety or 5% < P ≤ 10% for risks with primary impact on cost, schedule or performance
Very Low	1	**Qualitative:** Very unlikely to occur, management not required in all cases; strong controls in place **Quantitative:** P ≤ 10^{-5} for risks with primary impact on safety or P ≤ 5% for risks with primary impact on cost, schedule or performance

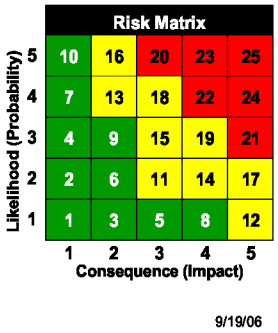


Figure 5 – Ares Risk Scorecard (ref. 13)

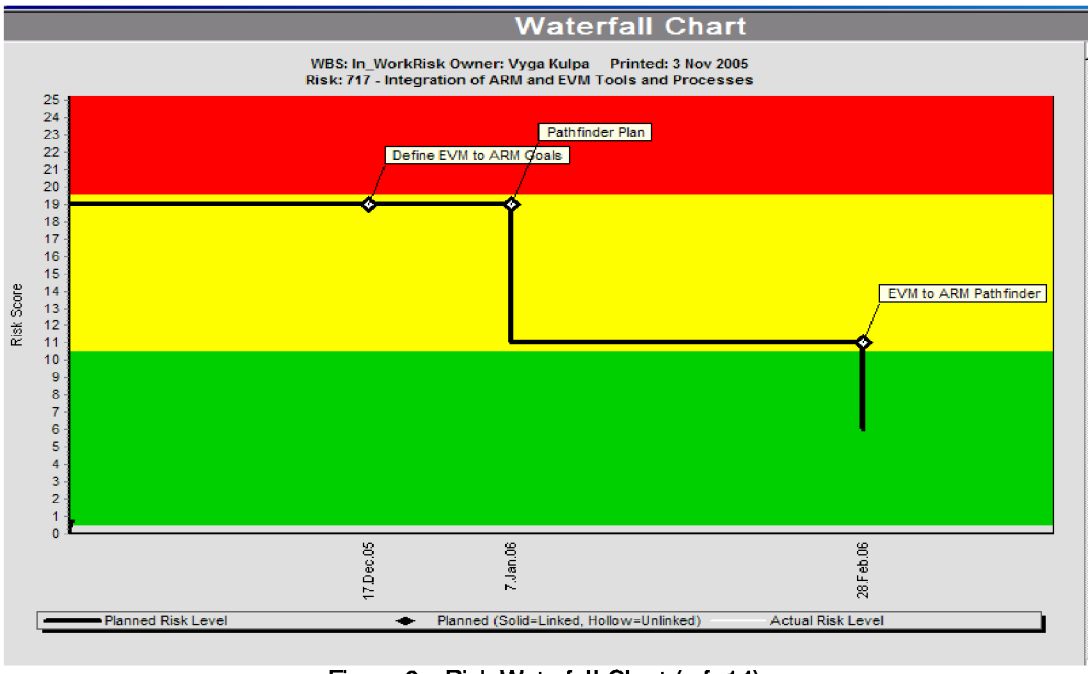


Figure 6 – Risk Waterfall Chart (ref. 14)

Summary of Improving Our Odds: Success Through CRM

While designing a rocket intended to launch humans into space is an extremely complex enterprise and while crossing a street is a simple routine effort, both endeavors can and should be preceded with an assessment of risk. Failure to do so in either case could lead to catastrophic results. Sometimes we fail to recognize risk, other times we recognize risk but disregard the steps to mitigate it even though the consequences may be significant. The application of the risk management process is effective in structuring our efforts to lessen the likelihood and/or the severity of risks we face. To persons in different situations, risk management takes on a different emphasis, yet the basics are the same. The philosophy and ideals of CRM can be beneficially applied to all situations. As noted, the risk management structure of identify, analyze, plan, track and control for dealing with risk can be used intentionally and in very involved ways or it can be applied subconsciously in simply situations, either way it will improve our odds of success.

References

1. American Heritage Dictionary of the English Language, William Morris Editor, Houghton Mifflin Company, Boston, Massachusetts, 1976, p. 1121

2. Audrey J. Dorofee, Julie A Walker, Christopher J. Alberts, Ronald P. Higuera, Richard L. Murphy, Ray C. Williams, Continuous Risk Management Guidebook, Carnegie Mellon University, 1996, p. 20

3. Audrey J. Dorofee, Julie A Walker, Christopher J. Alberts, Ronald P. Higuera, Richard L. Murphy, Ray C. Williams, Continuous Risk Management Guidebook, Carnegie Mellon University, 1996, p. 22

4. Audrey J. Dorofee, Julie A Walker, Christopher J. Alberts, Ronald P. Higuera, Richard L. Murphy, Ray C. Williams, Continuous Risk Management Guidebook, Carnegie Mellon University, 1996, p. 22

5. Audrey J. Dorofee, Julie A Walker, Christopher J. Alberts, Ronald P. Higuera, Richard L. Murphy, Ray C. Williams, Continuous Risk Management Guidebook, Carnegie Mellon University, 1996, p. 25

6. Audrey J. Dorofee, Julie A Walker, Christopher J. Alberts, Ronald P. Higuera, Richard L. Murphy, Ray C. Williams, Continuous Risk Management Guidebook, Carnegie Mellon University, 1996, pp. 24, 25

7. Wayne Hale, NASA Space Shuttle Program Manager, Letter to the NASA Space Shuttle Team from Wayne Hale on Risk, NASA, Johnson Space Center, October 26, 2004.

8. CxP 72019 (NASA, Constellation Program document), Exploration Launch Projects Risk Management Plan, June 21, 2006, p. 11

9. Phillip O. Greenhalgh, "Use of System Safety Risk Assessments for the Space Shuttle Reusable Solid Rocket Motor", Journal of System Safety 38, No. 1 First Quarter 2002, pp 12-17

10. CxP 72019 (NASA, Constellation Program document), Exploration Launch Projects Risk Management Plan, June 21, 2006, p. 26, Section 4.2

11. CxP 70043 (NASA, Constellation Program document), Constellation Program Failure Modes and Effects Analysis and Critical Items List (FMEA/CIL), NASA, 6 October 2006, p. 9

12. Phillip O. Greenhalgh, "Use of System Safety Risk Assessments for the Space Shuttle Reusable Solid Rocket Motor", Journal of System Safety 38, No. 1 First Quarter 2002, p. 12 - 17

13. CxP 72019 (NASA, Constellation Program document), Exploration Launch Projects Risk Management Plan, June 21, 2006, pp. 27 - 30, Figures 4.2.1-1, 4.2.1-2, 4.2.5-1

14. CxP 72019 (NASA, Constellation Program document), Exploration Launch Projects Risk Management Plan, June 21, 2006, p. 33, Figure 4.3.2.5-1

Biographical Sketch:

Phillip O. Greenhalgh, 437 West 200 South, Brigham City, UT 84302, Project Engineer, System Safety and Reliability, ATK Launch Systems Inc. Inc., P.O. Box 707, Brigham City, UT 84302, USA, telephone (435) 863-5438, facsimile (435) 863-2884, e-mail – phillip.greenhalgh@atk.com

Phil has enjoyed a career of over 24 years at ATK Launch Systems Inc. in Northern Utah as a system safety and reliability engineer working on solid rocket fuel propulsion systems. Phil is presently the lead engineer for System Safety and Reliability on the Ares I First Stage program. After completing a master's degree in safety at Central Missouri State University in 1985, he began his career at ATK (then Morton Thiokol). For 21 years, Phil worked on the Space Shuttle Solid Rocket Motor and Reusable Solid Rocket Motor programs also as a system safety and reliability engineer. He presently serves as the Risk Management Officer for the Ares I First Stage program at ATK. Phil has previously served as a contractor member of the NASA System Safety Review Panel. Phil joined the System Safety Society in 1987 and has published several papers on topics of system safety and risk management which were included in the proceedings of International System Safety conferences as well as the Journal of System Safety. Phil has been a Certified Safety Professional (CSP) since 1996.

A premier aerospace and defense company

Improving Our Odds:
Success Through Continuous Risk Management

Presented by: Phillip O. Greenhalgh

International System Safety Conference 2009
3 – 7 August 2009
Huntsville, Alabama

Improving Our Odds: Success Through Continuous Risk Management

A premier aerospace and defense company

- **RISK** is always present in everything we do be it a simple act or a major, complex operation:
  - Crossing a Street
    - Video Clip of Man crossing street
  - Launching a Rocket
    - ATK DVD “Vision – Innovation- Execution”
- We Can **Improve our odds of success through Continuous Risk Management**
  - **Risk Management** can be used for simple processes in an unconscious manner to make us safer. Is almost imperative to use for large enterprises if risk is to be reduced to acceptable levels
- **Risk Management** is the structure for dealing with risk, be it intentional and involved or subconscious and simple.
- **Risk Management** is "a discipline for living with the possibility that future events may cause adverse effects”

"It ain't what you don't know that gets you into trouble. It's what you know for sure that just ain't so."

Mark Twain

"You've got to be very careful if you don't know where you're going, because you might not get there."

Yogi Berra

Risk Management

Risk Management PREDICTS, and then mitigates events that could prevent us from reaching our objectives. Our other measures of performance look in the "rear-view mirror" to see what HAS happened and, therefore, do nothing to prevent risks from coming to pass.

Risk Management is a culture, a way of doing business, and a duty of all program, functional members and stakeholders. It is not a tool, a place, or a person. It is a continuous process shared by all program and functional personnel to capture, communicate and mitigate risks over the life of a program or function.

The Continuous Risk Management Process

Risk Management Process

Identify – find the risks before they can become problems and result in loss or harm. A process of realizing the uncertainty for loss or harm

- Capture the statement of risk in a way it can be described and measured
  - Given the (condition) there is a potential that (risk) could result in (consequence)
- Capture the context of risk
  - Include additional information relevant to the circumstances surrounding the identified risk
- Communicate the identified risk
  - Communicate – Communicate - Communicate

Examples of communicating Risk

Poor

These risk statements are too general. They are concerns, certainly, but don't give enough specifics to tackle in a meaningful way

"Given the complexity of the vehicle there is a potential for errors to occur which could result in disaster."

"Given the dynamics of the program, there is a potential for inaccurate flow downs and interface breakdowns, which could result in costly/evolving changes"

"Given the overall vehicle complexity, there is a potential for safety or quality disconnects, which could adversely affect performance, mission completion or result in system failure."

Better

These risk statements or more specific and will help focus mitigation planning

"Given the potential for error in the results of the random vibration analysis, there is a potential of underestimating the environment, which could result in a failure to verify avionics boxes to their flight environment leading to the worst case scenario of flight failure."

"Given the potential for errors in the structural dynamics predictions there is a potential for incorrect vehicle modes which could result in loss of vehicle (structural breakup, fluid exhaustion, etc).

"Given that we have specified stages and have not established design to cost metrics, there is a potential that the vehicle may carry too high an inert weight to payload fraction, resulting in degraded market potential."

Improving Our Odds: Success Through Continuous Risk Management

Analyze – process of examining the risk in order to tell the potential extent, severity and likelihood

- Evaluate the attributes of risks
  - Impact
  - Probability
  - Timeframe
- Classify the risks
  - Grouping of risks based on similar characteristics
- Prioritize the risks
  - Ranking of risks to define those most significant or those that need the most attention
- Communicate the results or status of the analysis

Plan – decide what to do with risks and how to go about doing it

- Plan risk mitigation activities
- Assign responsibilities
- Communicate what is happening with the risk and how it is going

Improving Our Odds: Success Through Continuous Risk Management

Track/Document – follow the risk and the assigned risk responsibilities, collect more information

- Monitor the risk and all related actions
- Provide status reports
- Communicate information relative to the progress of the risk

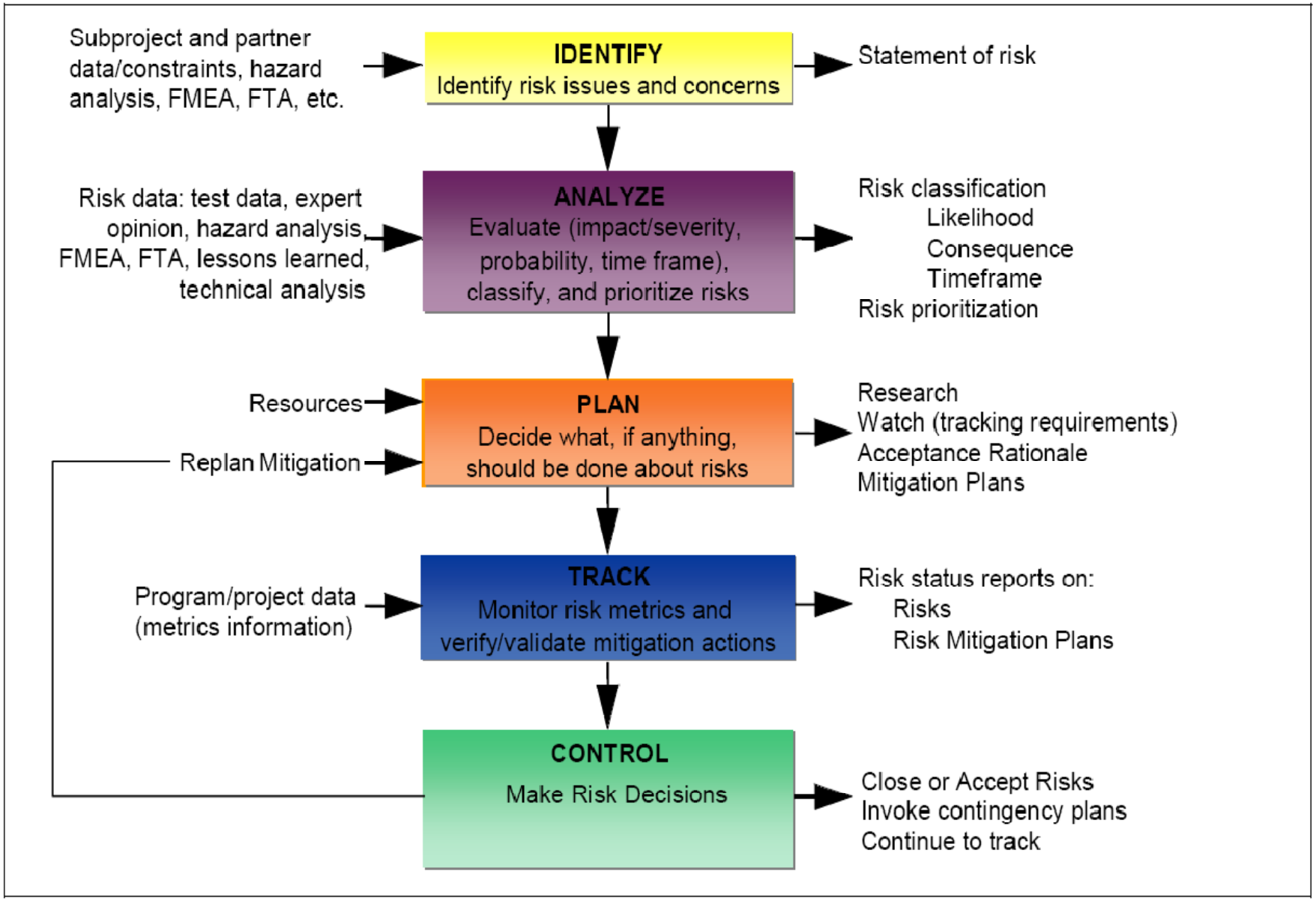
Control – executing the risk mitigation activities that will reduce risks to levels where the uncertainties (likelihood) and potential loss (severity) are reduced to an acceptable level

- Implement the controls
- Monitor the controls
- Communicate the effectiveness of the controls

- COMMUNICATION is the centerpiece that holds the Continuous Risk Management process togeth

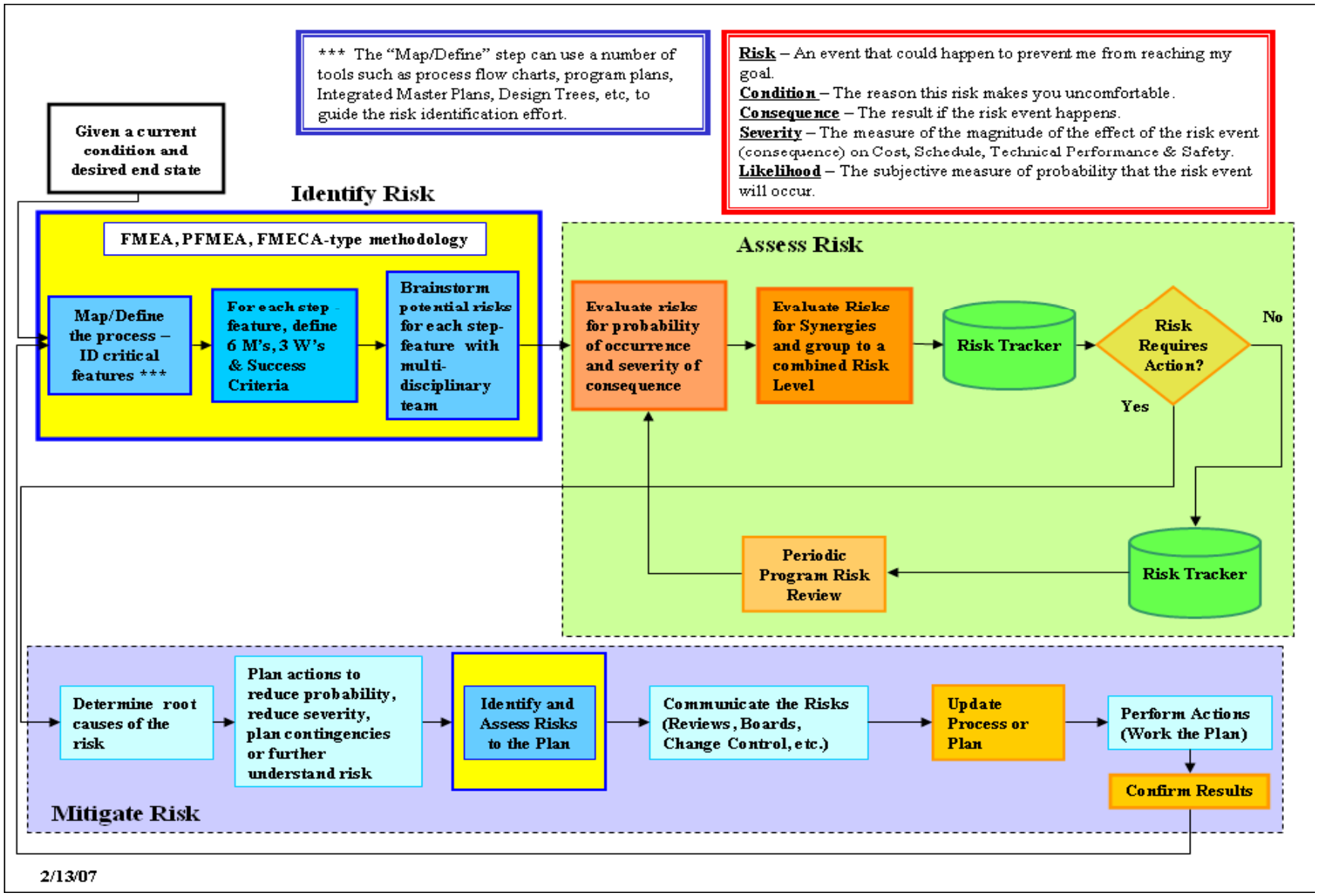
Improving Our Odds: Success Through Continuous Risk Management

A premier aerospace and defense company



Improving Our Odds: Success Through Continuous Risk Management

A premier aerospace and defense company



Improving Our Odds: Success Through Continuous Risk Management

A premier aerospace and defense company

Continuous, Life Cycle Risk Management:
Risk-based Design
Program Risk, Product Hardware Risk, Process Risk, Support Process Risk, Facility and Process Risk, Supplier Risks, Other Risks

Advanced Risk Management Tools: Reliability Analysis, PRA, FMEA/RECA, FMECA, PFMEA/PRECA, Brainstorming, ETC.

Definitions

Risk – A credible future event that would prevent you from reaching a goal or objective – something that could go wrong with a planned activity (Problem vs. Risk)

Risk Level – A combination of the likelihood that a risk will happen, with the severity of its consequence if it does happen – Consequences are typically categorized as to Safety, Cost, Technical and/or Schedule

Mitigation – A planned, scheduled and funded action to reduce the likelihood or severity of a risk

(An unplanned, unfunded, unscheduled action is could be called a hallucination)

Assess Risks - Likelihood

Not “worst conceivable case”

Determination of risk is for “worst credible case”

Not “best case” (all success type)

Likelihood / Probability can be either quantitative or qualitative

- Qualitative
  - Subjective Evaluation based on a Simple Scale
    - i.e. – “Remote” to “Near Certain” “1-5”
- Quantitative
  - Probability Risk Assessment (PRA)
  - Reliability Analysis
  - Event Sequence Analysis
  - Statistical Probability based on Historical Data
  - Etc.

Assess Risks - Severity

Not “worst conceivable”

Determination of risk is for “worst credible case”

Not “best case” (all case success type)

Severity is qualitative

If words on card do not match your need, change them

What is required is a gradation – from minor to catastrophic

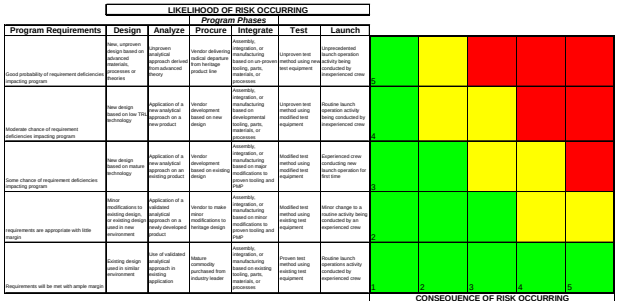
FMECA, HA, PHA, Crit 1, Crit 1R, Crit 2, Crit 3 designations

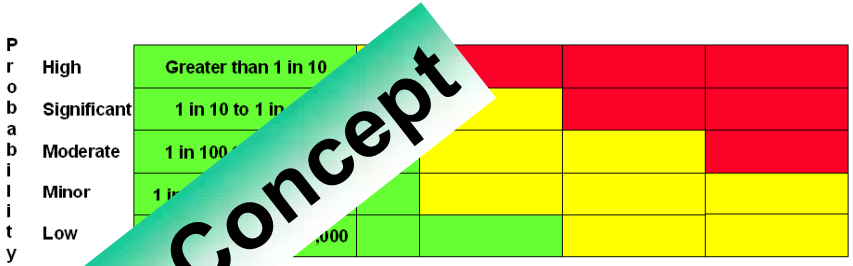
are all tools, but still use subjective evaluations (peer reviewed, rigorous process)

Likelihood x Severity (Risk) “number” allows us to place challenges in a gross prioritization which is used for resource prioritization

Improving Our Odds: Success Through Continuous Risk Management

A premier aerospace and defense company





Many Definitions but One Concept

LIKELIHOOD RATING

5	Very High	Qualitative: Nearly certain to occur. Controls have little or no effect. Quantitative: ~10-1
4	High	Qualitative: Highly likely to occur. Controls have significant uncertainties. Quantitative: ~10-2
3	Moderate	Qualitative: May occur. Controls exist with some uncertainties. Quantitative: ~10-3
2	Low	Qualitative: Not likely to occur. Controls have minor limitations/uncertainties. Quantitative: ~10-4
1	Very Low	Qualitative: Very unlikely to occur. Strong Controls in Place Quantitative: ~10-5

CxP Risk Summary C...

eframe	
	0 to 3 months
Mid	>3 Months but <9 months
Far	>9 months

Consequence		1			4	5
Safety	Personnel	Minor first aid treatment though would not adversely affect personal safety or health	Mi...	...l injury or ...ess	Permanently disabling injury	Death or loss of crew
	System Safety	Minor damage to secon... Or non-essential flig...		...age to flight assets, or ...Damage to Program critical ...ets, or loss of non-essential ...assets	Major damage to flight assets, Or loss of Program critical assets	Loss of flight assets
	Environmental	Negligible OSHA/EP... Non-reportable		Moderate OSHA/EPA violation which requires immediate remediation	Major OSHA/EPA violation causing temporary stoppage	Serious or repeat OSHA/EPA violations resulting in action terminating project
Performance (mission success)	Requirements	Negligible impact to requirements/design margins		...ign Moderate impact to requirements/design margins	Major impact to requirements/design margins	Technical goals not achievable with existing engineering capabilities/technologies
	Operations	Negligible impact to mission objectives/operations	N... ...l impact to operations – workarounds available	Moderate impact to operations – workarounds available	Failure to achieve major mission objectives	Contingency Abort
	Supportability	Temporary usage loss or LOCM of non-flight critical asset	Permanent usage loss or LOCM of non-flight critical asset	Temporary usage loss or LOCM of major element(s) of flight vehicle or ground facility	Permanent usage loss or LOCM of major element(s) of flight vehicle or ground facility	Inability to support further CxP flight operations
Cost (Estimate to Complete)		≤ 2% -Or- < $100 K	>2%, but ≤5% -Or- $100 K - $1 M	>5%, but ≤10% -Or- $1 M - $10 M	>10%, but ≤15% -Or- $10 M - $50 M	>15% -Or- > $50 M
Schedule		Negligible schedule impact	Minor overall schedule impact (Accommodate with reserve, no impact to critical path)	≤ 1 month delay to Program/Project milestone (SRR, PDR, CDR, SAR)	>1 and ≤5 month Program/Project critical path/milestones (SRR, PDR, CDR, SAR)	>5 month delay to Major Program critical path/milestones or can not meet major milestones (SRR, PDR, CDR, SAR)

CxP 70056, Cx Program Risk Management Plan

Frequency of Occurrence	Hazard Severity (1) Catastrophic	(2) Critical	(3) Marginal	(4) Negligible	
(A) Frequent	1A	2A	3A	4A	A
(B) Probable	1B	2B	3B	4B	B
(C) Occasional	1C	2C	3C	4C	C
(D) Remote	1D	2D	3D	4D	D
(E) Improbable	1E	2E	3E	4E	E
	1	2	3	4	

Why look at Risk Synergies?

Individual risks can stack up to be more significant than they might appear individually

If only look individually may mis-prioritize and not commit resources where they are most critical

Example 1: Single poisonous snake in a large yard – risk

2nd single poisonous snake (SPS) in a large yard – risk

3rd, 4th, 5th, 6th SPS in a large yard – low risk

6 poisonous snakes in a large yard – low risk to me, I'm staying away from that yard together very high risk

May seem obvious, but six different schedule risk items are often assessed as low risk individually. The combination of these can be catastrophic to a Program and need to be assessed (appropriate) for mitigation that way.

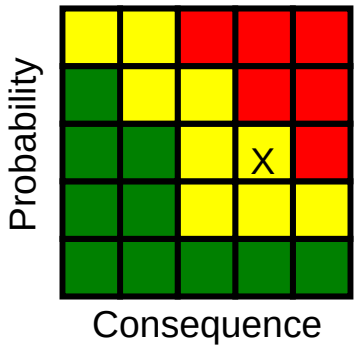
Cost risks can be the same.

Capacity planning can be the same.

What should synergy look like?

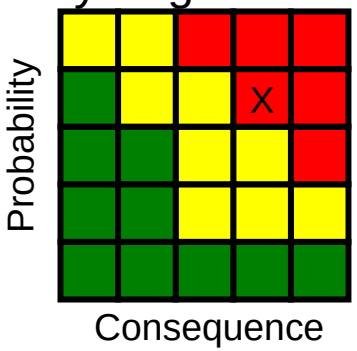
1,2,3, 22				
19,20, 21,	4		5,23, 29	
35,36	18	17	6,7,10 11,25, 28, 38	
	8,15, 31,32, 33	13,14 16,24, 34	9,12, 26, 27,30, 37, 39	

Individual Risks



1,2,3, 22			5,23,7, 25, 10, 28, 11, 29	
19,20, 21,	4			
35,36	18	17	6,38	
	8,15, 31,32, 33	13,14 16,24, 34	9,12, 26, 27,30, 37, 39	

Risk Synergies Considered



To Mitigate (ALL red risks and red synergies and selected yellow / green):

A. Understand root cause of risk
B. Employ ALL of the following:

    1) Consider mitigations that reduce either likelihood

    2) Consider mitigations that reduce either severity

    3) Consider mitigations that are reactive to the risk being realized i.e. contingency plans (i.e. coming back on line, hang-fire planning, recovery after an earthquake)

    4) Analysis actions (define the actions that will enable understanding so that mitigation plans can be more effective – Informed decision making)

C. Mitigate risk synergies as required for highest Program benefit
D. Create a funded, scheduled activity that is tracked as part of program plan – risks mitigations are to below red levels – how far below is a Program decision

What Risk Mitigation is Not

Analysis doesn't change risk if hardware, resources, requirements or tools are not changed – exception: risk of having an unknown (which generally isn't useful to track except for having a >10% Program reserve at initiation of a properly funded Program)

Getting through a review is not a risk mitigation

An unfunded, unscheduled, albeit thought-out approach, is not a risk mitigation

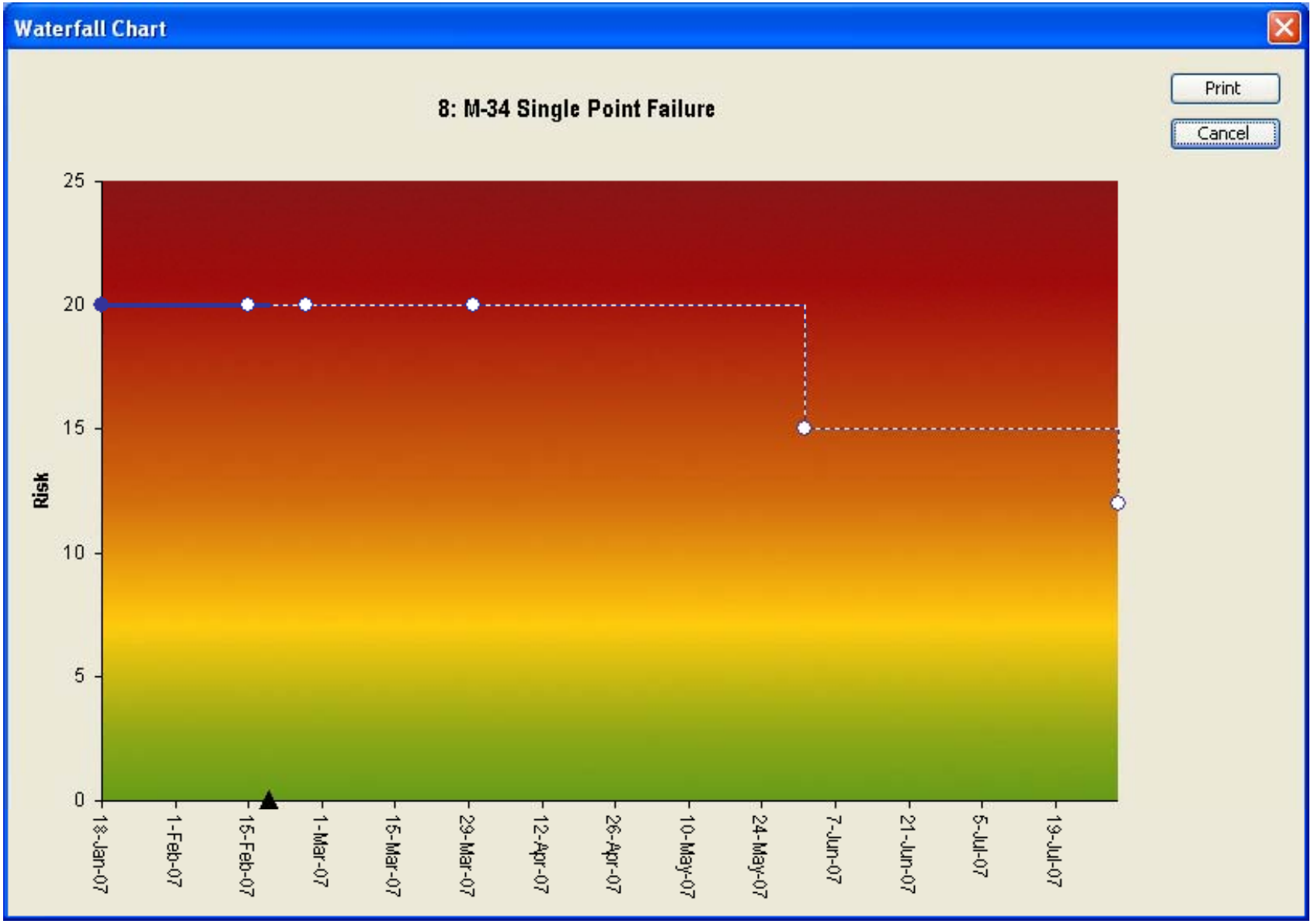
Changing a risk number due to Programmatic / Functional pressures, without new data, or merely deciding to accept a level of risk is not mitigation

Mitigating a direct / immediate cause, without mitigating the root cause is not an effective mitigation

Out waiting the risk item (finding out in test if performance is acceptable) is not a mitigation

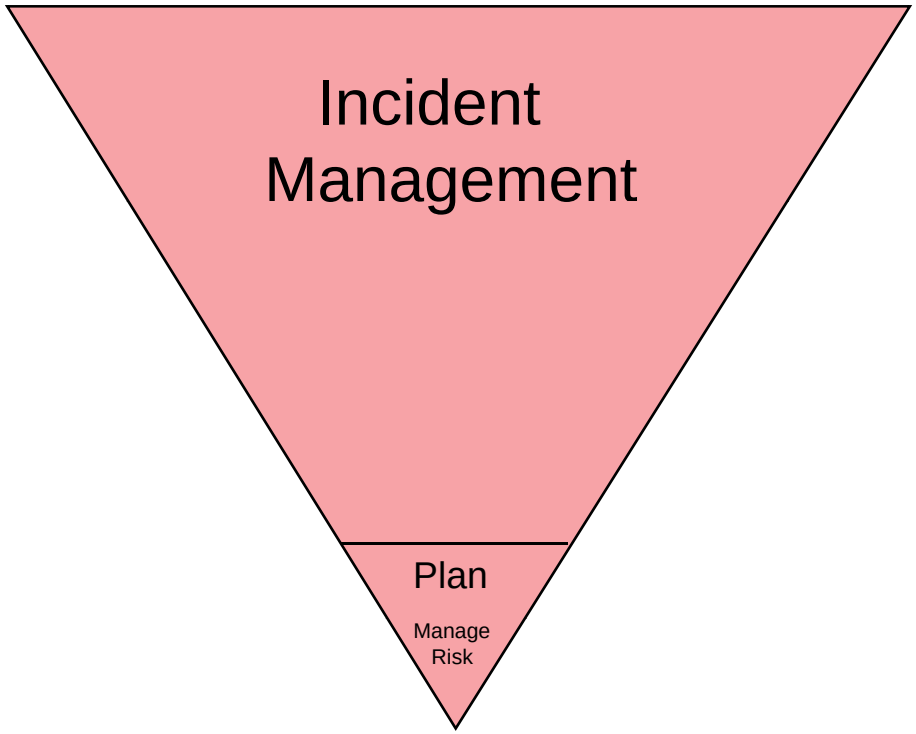
Improving Our Odds: Success Through Continuous Risk Management

A premier aerospace and defense company



Improving Our Odds: Success Through Continuous Risk Management

- RISK is present in everything we do be it a simple act or a major, complex operation. We can choose to over look risks and manage the consequences when they become incidents:



- OR -

Improving Our Odds: Success Through Continuous Risk Management

A premier aerospace and defense company

We can use the Continuous Risk Management Model to Improve Our Odds of Being Successful and Avoiding Loss